Consensus Audit Guidelines: Time to "Stop The Bleeding"

John M. Gilligan

10th Semi-Annual Software Assurance Forum

March 12, 2009

Topics

- Background
- Philosophy and Approach for the Consensus Audit Guidelines (CAG)
- CAG Examples and List of Controls
- CAG Next Steps
- Final thoughts

Cyber Security Today—A New "Ball Game"

- Our way of life depends on a reliable cyberspace
- Intellectual property is being downloaded at an alarming rate
- Cyberspace is now a warfare domain
- Attacks increasing at an exponential rate
- Fundamental network and system vulnerabilities cannot be fixed quickly
- Entire industries exist to provide "Band Aids" for engineering and operational weaknesses

Cyber Security is a National Security Crisis!

Government Security Environment

- We are in a cyber war and we are losing badly!
- The IT industry has produced an inherently unsecure environment
- CIO mandates exceed time and resources available
- Cyber security is an enormously complex challenge—there are very few true experts

It is time to focus on ways to make real improvements in security

FISMA—Well Intended; What is Not Working??

- Original intent was good:
  - Ensure effective controls
  - Improve oversight of security programs
  - Provide for independent evaluation
- Implementation took us off course
  - (Lots of) NIST general "guidance" became mandatory
  - No auditable basis for independent evaluation
  - Grading became overly focused on paperwork

Increased cost and lots of debates about real security improvements

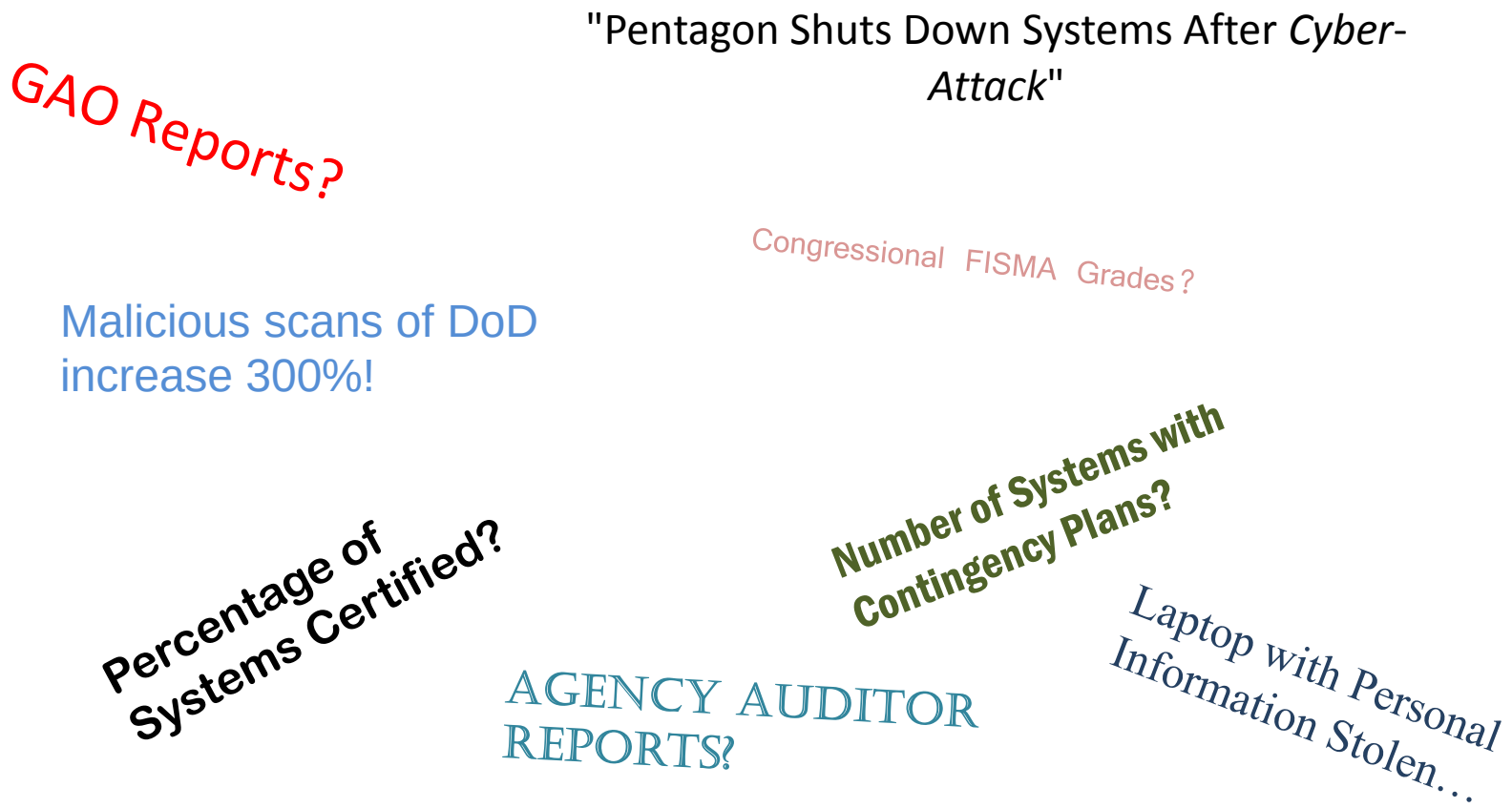
Analogy of Current FISMA Implementation

- An ambulance shows up at a hospital with bleeding patient
- Hospital gives inoculations for flu, tetanus, shingles, vaccination updates
- Hospital tests for communicable diseases, high blood pressure, sends blood sample for cholesterol check, gives eye exam and checks hearing
- At some point, doctors address the cause of the bleeding

Meanwhile, the patient is bleeding to death!!

We Need Triage--Not Comprehensive Medical Care

How Should We Assess Effective Security



We need to objectively measure the effectiveness of security controls!

Consensus Audit Guidelines Philosophy

- Leverage cyber offense to inform cyber defense – focus on high payoff areas
- Ensure that security investments are focused to counter highest threats — pick a subset
- Maximize use of automation to enforce security controls — negate human errors
- Use consensus process to collect best ideas

Focus investments by letting cyber offense inform defense!

Approach for developing CAG

- Engage the best security experts:
  - NSA “Offensive Guys”
  - NSA “Defensive Guys”
  - DoD Cyber Crime Center (DC3)
  - US-CERT (plus 3 agencies that were hit hard)
  - Top Commercial Pen Testers
  - GAO
  - Top Commercial Forensics Teams
  - JTF-GNO
  - AFOSI
  - Army Research Laboratory
  - DoE National Laboratories
  - FBI and IC-JTF
- Prioritize controls to match successful attacks
- Describe automation/verification methods
- Engage CIOs, CISOs, Auditors, and Oversight organizations
- Coordinate with Congress regarding FISMA updates

CAG Example--Critical Control #1
Inventory of authorized and unauthorized hardware

- **Attacker Exploit**: Scan for new, unprotected systems
- **Control**: Accurate, up to date inventory controlled by automated monitoring and configuration management
- **Automated Support**: Employ products available for asset inventories, inventory changes, network scanning against known configurations
- **Evaluation**: Connect fully patched and hardened machine to test response from automated tools

CAG Example--Critical Control #2
Secure Configurations for Hardware and Software
(where such configurations are available)

- **Attacker Exploit**: Automated search for improperly configured* systems
- **Control**: Deploy "locked down" configurations
- **Automated Support**: Employ SCAP and similar tools to monitor/validate configurations
- **Evaluation**: Introduce improperly configured system to test response times/actions

* Incorrectly configured or using manufacturer settings

Consensus Audit Guidelines

(Critical Controls Subject to Automated Verification--1 thru 15)

1. Inventory of authorized and unauthorized hardware.
2. Inventory of authorized and unauthorized software.
3. Secure Configurations for Hardware and Software For Which Such Configurations Are Available.
4. Secure Configurations of Network Devices Such as Firewalls And Routers.
5. Boundary Defense
6. Maintenance and Analysis of Complete Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based On Need to Know
10. Continuous Vulnerability Testing and Remediation
11. Dormant Account Monitoring and Control
12. Anti-Malware Defenses
13. Limitation and Control of Ports, Protocols and Services
14. Wireless Device Control
15. Data Leakage Protection
16. Secure Network Engineering
17. Red Team Exercises
18. Incident Response Capability
19. Disaster Recovery Capability
20. Security Skills Assessment and Training To Fill Gaps

Next Steps

- Refine CAG document—public comment period through March 25th.
- Continue outreach effort to CIOs, CISOs, Auditors/IGs
  - Identify FY '09 government pilot sites
  - Develop recommendations regarding policy implementation and "scoring" approach
- Workshops on specifications for tools for each CAG control (Starting late April)

Final Thoughts

- A well managed system is a harder target and costs less to operate
- Federal government actions can lead global change
- In the near-term we must focus our efforts to make measurable progress

We Need to Stop the Bleeding—Now!

Contact Information

John M. Gilligan

jgilligan@gilligangroupinc.com
www.gilligangroupinc.com

Backup

Cyber Security Commission

- Structure
  - Congressional sponsorship; managed by CSIS
  - Broad government, industry, and academic expertise and close coordination with CNCI
- Observations
  - Leadership must focus on National Security issue
  - Technology and governance lagging needs

Objective: "Game Changing" recommendations

Cyber Security Commission Recommendations

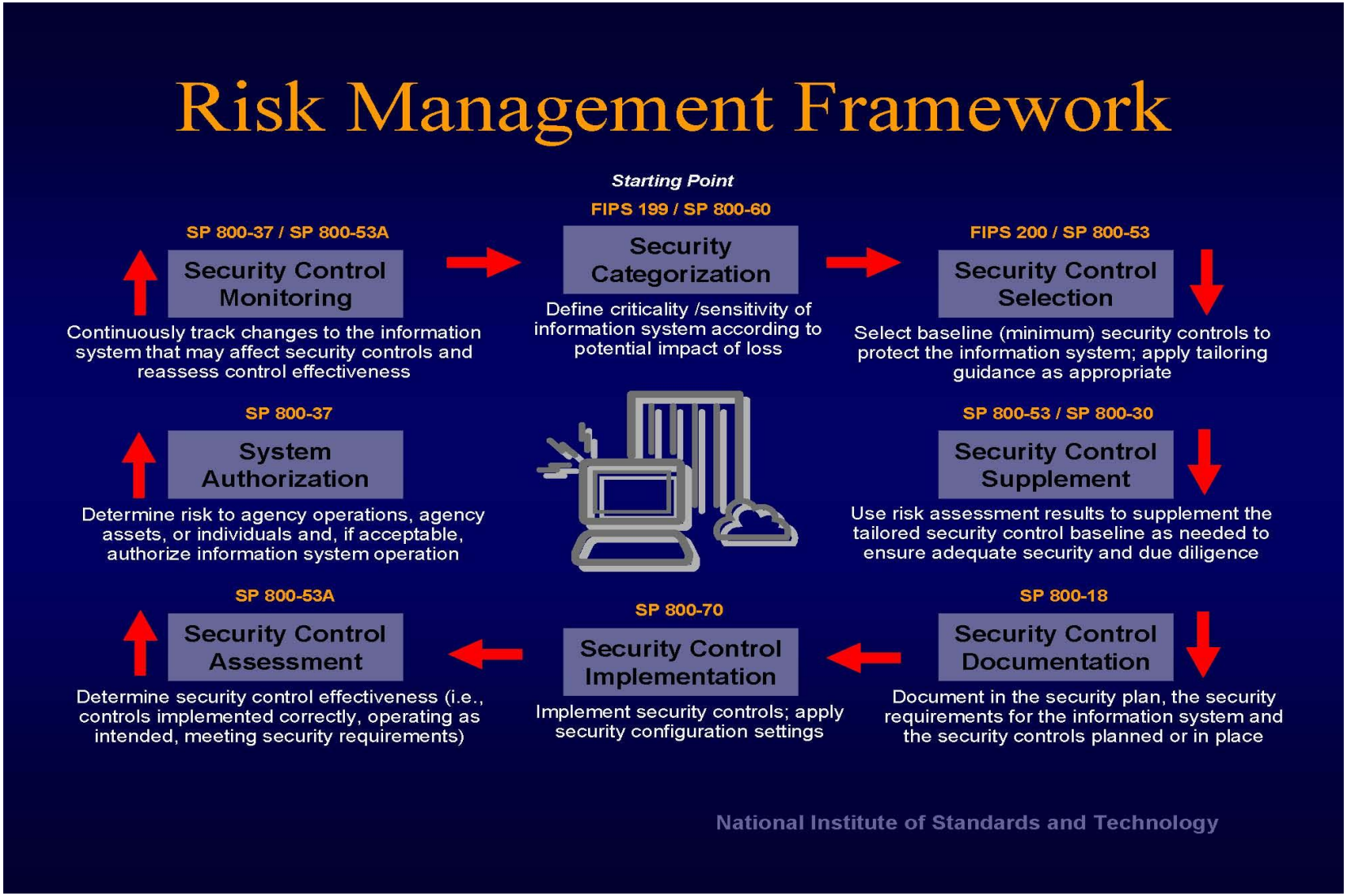
- Develop National Strategy for Cyberspace and publish National Cyberspace Doctrine
- Elevate and consolidate authorities for cyberspace (to White House)
- Enhance partnership with private sector
- Leverage elevated authority to coordinate existing regulatory authorities
- Use federal acquisition authorities to change industry model
- Modernize legal and policy framework

FISMA Original Intent

- Framework to ensure effective information security controls
- Recognize impact of highly networked environment
- Provide for development and maintenance of minimum controls
- Improved oversight of agency information security programs
- Acknowledge potential of COTS capabilities
- Selection of specific technical hardware and software information security solutions left to agencies
- Provide independent evaluation of security program

However: FISMA has evolved to "grading" agencies based largely on secondary artifacts

Risk Management Framework



NIST Guidance: 1200 pages of FIPS Pubs, Special Pubs, Security Bulletins, etc.

NIST Security Guidance

- NIST Risk framework consists of over 1200 pages of guidance
- An additional security-related mandatory 15 Federal Information Processing Standard (FIPS) Publications
- Over 100 additional security related special publications
- Over 35 Interagency Reports
- Over 65 Security Bulletins (since 2002)

A very impressive list of guidance—but is it contributing to improved security?